

STEPTOE & JOHNSON LLP

ATTORNEYS AT LAW

1330 CONNECTICUT AVENUE, N.W.
WASHINGTON, D.C. 20036-1795

PHOENIX, ARIZONA
TWO RENAISSANCE SQUARE

TELEPHONE: (602) 257-5200
FACSIMILE: (602) 257-5299

JAMES M. TALENS
(202) 429-8177
jtalens@steptoe.com

(202) 429-3000

FACSIMILE: (202) 429-3902

TELEX: 89-2503

STEPTOE & JOHNSON INTERNATIONAL
AFFILIATE IN MOSCOW, RUSSIA

TELEPHONE: (011-7-501) 258-5250
FACSIMILE: (011-7-501) 258-5251

DOCKET FILE COPY ORIGINAL

April 14, 1998

RECEIVED

APR 14 1998

BY HAND DELIVERY

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

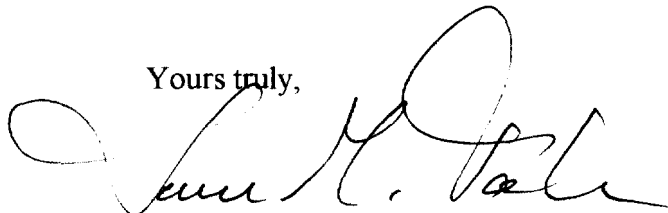
**Re: Further Notice of Proposed Rulemaking in CC Docket No. 96-115,
Implementation of the Telecommunications Act of 1996;
Telecommunications Carriers' Use of Customer Proprietary Network
Information and Other Customer Information**

Dear Ms. Salas:

Enclosed for filing are an original and eleven copies of the Reply Comments of Iridium North America in the above-referenced proceeding. Please date stamp and return the additional enclosed copy.

Please call me if you have any questions.

Yours truly,



James M. Talens

Counsel for Iridium North America

Enclosures

No. of Copies rec'd
List ABCDE

0411

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

RECEIVED

APR 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)

Implementation of the)
Telecommunications Act of 1996;)
Telecommunications Carriers' Use of)
Customer Proprietary Network Information)
and Other Customer Information)
_____)

CC Docket No. 96-115

REPLY COMMENTS OF IRIDIUM NORTH AMERICA

Philip L. Malet
James M. Talens
Tekedra V. McGee

Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 429-3000

Counsel for Iridium North America

April 14, 1998

TABLE OF CONTENTS

	<u>PAGE</u>
I. The Commenters Agree that the FBI's Proposal to Limit Storage of and Foreign Access to CPNI is Unnecessary and Overreaching.....	2
II. The Commission Must Not Make National Policy Limiting Storage and Access to Customer Data in the Absence of Congressional Action or Express Congressional Intent.....	4
III. Conclusion	6

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)
)
)

Implementation of the)
Telecommunications Act of 1996;)
Telecommunications Carriers' Use of)
Customer Proprietary Network Information)
and Other Customer Information)
_____)

CC Docket No. 96-115

To: The Commission

REPLY COMMENTS OF IRIDIUM NORTH AMERICA

Iridium U.S., L.P. ("Iridium North America" or "INA")¹ hereby submits its reply comments in support of the initial comments in the above-captioned proceeding.²

The comments overwhelmingly oppose the Federal Bureau of Investigation's ("FBI") proposal to limit storage of and access to Customer Proprietary Network Information ("CPNI") to the United States. The Commenters agree with INA that there is no justification in the law or Congressional intent for interpreting new Section 222 of the Communications Act of

¹ INA is a limited partnership owned by subsidiaries of Motorola, Inc., Sprint Corporation and BCE, Inc. (Canada's largest telecommunications company). Each of these partners is an investor in Iridium LLC. Iridium LLC has allocated INA the North American gateway service territory, consisting of Canada, Bermuda, Puerto Rico and the U.S. The Commission recently granted INA Section 214 authority to serve all international points from the U.S. via the Iridium[®] System. (See FCC File No. ITC-97-697).

² In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, Second Report and Order and Further Notice of Proposed Rulemaking in CC Docket 96-115 (rel. Feb. 26, 1998).

1934, as amended,³ as a basis for establishing new national data storage policy. Accordingly, the Commission should reject the FBI's proposal.

I. The Commenters Agree that the FBI's Proposal to Limit Storage of and Foreign Access to CPNI is Unnecessary and Overreaching

Commenters in this proceeding agree with INA that carriers must comply with Section 222 and that Section 222 of the Act provides adequate protection for CPNI, regardless of where the such information is stored.⁴ The FBI assumes that Section 222 is inadequate to protect CPNI and that there is a need for the Commission to micro-manage telecommunications carriers. There is no basis for this assumption on the record. The FBI's proposal would disrupt the ordinary business operations of telecommunications service providers. If adopted, as MCI correctly states, the FBI's proposal would leave "U.S. carriers . . . ultimately . . . handicapped in the emerging global competition among multinational carriers."⁵

Global telecommunications companies, such as INA and Omnipoint Communications, Inc., are not capable of complying with the FBI's proposed limitations. As discussed in INA's comments, the global sharing of CPNI is integral to the roaming operations of the Iridium[®] System.⁶ Accommodating the FBI's proposal would require redesigning and restructuring the entire Iridium[®] System, a virtual impossibility. Similarly, Omnipoint's

³ 47 U.S.C. § 222.

⁴ See GTE Comments at 7-8; Comments of MCI Telecommunications Corporation at 17-20 ("MCI Comments"); Comments of Omnipoint Communications Inc. at 2, 6-11 ("Omnipoint Comments"); AT&T Comments at 4 n.6; Comments of Intermedia Communications, Inc. at 10-12 ("Intermedia Comments").

⁵ MCI Comments at 18-19.

⁶ See INA Comments at 7-9.

comments clearly demonstrate that the FBI's proposal would present major obstacles to the provision of international commercial mobile radio service ("CMRS") and CMRS roaming services.⁷ In that regard, Omnipoint states that "[a] rule prohibiting foreign carriers from obtaining direct carrier access to CPNI used in roaming would make international GSM nearly impossible."⁸ Omnipoint also recognizes that the FBI's proposed restrictions could result in foreign retaliation, creating even greater obstacles to the provision of international service.⁹

Other carriers have similar concerns. AT&T indicates that its services require access to CPNI by employees and affiliates located in foreign countries. Under the FBI's approach, however, AT&T would be unable to use CPNI for important operational purposes or to craft appropriate service offerings¹⁰ -- tasks integral to AT&T's business functions. For its part, Ameritech states that it would be severely impaired by the FBI's proposal to restrict foreign access to U.S.-stored CPNI.¹¹ While Ameritech does not store CPNI outside the U.S., it employs foreign firms for information systems development and production support. These tasks sometimes require incidental access to U.S.-located CPNI.¹² Restricting access would effectively force Ameritech, and others similarly situated, to completely reconfigure their business operations, without any perceivable benefit.

⁷ See Omnipoint Comments at 7-11.

⁸ Omnipoint Comments at 8.

⁹ See id.

¹⁰ AT&T Comments at 4 n.6.

¹¹ Comments of Ameritech at 1-2 ("Ameritech Comments").

¹² Id.

The FBI's proposal completely ignores the enormous business incentives telecommunications carriers already have in protecting their own CPNI.¹³ CPNI is, after all, one of the most valuable assets a carrier possesses. As long as a carrier's business prospects are linked to the security of its CPNI, and Section 222 reinforces the integrity of that security, there is no need for further regulatory protection or oversight. Indeed, as GTE correctly states, there is simply "[n]o evidence . . . that there is a need for the FCC to intervene in company decision-making when it comes to storage and protection of CPNI."¹⁴ Moreover, as Intermedia Communications, Inc. states, "[while] the FBI's desire for ready access to CPNI [is understandable], special record keeping requirements created solely to make CPNI available to law enforcement go beyond the scope of section 222, which is concerned solely with the carrier-customer relationship, not law enforcement access to customer records."¹⁵

II. The Commission Must Not Make National Policy Limiting Storage and Access to Customer Data in the Absence of Congressional Action or Express Congressional Intent

The FBI has asked the Commission to break new ground in regulating sensitive consumer data by expansively reading Section 222 to require domestic storage of and to limit foreign-carrier access to CPNI. However, Congress has not explicitly or implicitly indicated that the Commission -- or any other administrative agency -- should interpret the statute in a manner creating national data storage and/or access limits. In fact, where Congress has sought to

¹³ See Ameritech Comments at 1-3.

¹⁴ GTE Comments at 7.

¹⁵ Intermedia Comments at 11.

legislate in this area, it has directed its concerns solely to the uses of those data, never their storage location.

For example, Congress enacted the Federal Truth in Lending Act ("Act"), 15 U.S.C.A. §1601 et seq., in part, to "protect the consumer against inaccurate and unfair credit billing and credit card practices." 15 U.S.C.A. §1601(a). The Board of Governors of the Federal Reserve System thereafter issued regulations to implement that Act "to promote the informed use of consumer credit." 12 C.F.R. § 226.1(a). Neither the statute nor the promulgated regulations mandates a specific storage location for consumer credit records. In fact, the regulation regarding record retention makes clear that such regulation is principally concerned with ensuring that creditors comply with specified disclosure requirements, not with where records are physically stored.¹⁶

Similarly, Section 222 of the Act was enacted to protect consumers from unauthorized use and disclosure of CPNI. Congress did not seek to regulate the location of this information. Indeed, designating a particular storage location does not ensure authorized use or appropriate disclosure of CPNI. As GTE notes, a recent event involving a Department of Defense computer system has demonstrated that "physically locating sensitive data within this country is no guarantee that hackers will not be able to gain illegal access to the data."¹⁷

All parties in this rulemaking proceeding agree that carriers must protect CPNI. While the FBI offers alternative means of protecting this information, it fails to conclusively

¹⁶ See 12 C.F.R. § 226.25. The "[r]ecord retention" regulation, for example, states that "[a] creditor shall retain evidence of compliance with this regulation . . . for 2 years after the date disclosures are required to be made or action is required to be taken." 12 C.F.R. § 226.25 (a) (emphasis added).

¹⁷ GTE Comments at 8 n.10.

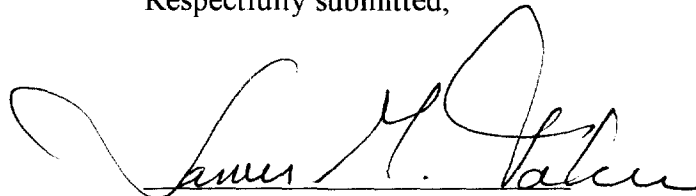
demonstrate that Section 222, in conjunction with the Commission's newly-adopted consumer protection rules, is inadequate to protect CPNI. Any party requesting the Commission to create a new national customer data policy must, at a minimum, demonstrate that current regulatory procedures are inadequate. Additionally, any proposal for the kind of pervasive data storage changes the FBI proposes must be solidly anchored in an express Congressional mandate or, at least, inferred from clear Congressional intent. In this case, they are not.

In the absence of any Congressional guidance, and because the FBI's proposal does not provide additional protective assurances for CPNI, the Commission must refrain from expanding the purpose of Section 222. The FBI's proposal for enhanced protection fails to warrant such a drastic departure from current national customer data policy.

III. Conclusion

For all the foregoing reasons, INA urges the Commission to reject the FBI's proposal regarding the storage of CPNI.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Philip L. Malet", written over a horizontal line.

Philip L. Malet
James M. Talens
Tekedra V. McGee

Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 429-3000

Counsel for Iridium North America

April 14, 1998